## CLAIMS

1. A method for authenticating a user by an identification center over a communication medium, comprising:

(a) sending via the communication medium an encryption key including at least an n for applying a function $Y=X^e \pmod n$ to a password of the user, wherein said password is presumed to be accessible to the user and to the identification center;

(b) the user encrypting said password using at least said encryption key;

(c) the user sending said encrypted password via the communication medium;

(d) the identification center receiving said encrypted password via the communication medium;

(e) the identification center simulating said encrypting on at least one of the passwords accessible to the identification center;

(f) the identification center comparing said at least one simulated encrypted password to said received encrypted password; and

(g) if results of said comparing are sufficient, the identification center sending via the communication medium an indication that the user has been authenticated.

2. The method of claim 1, wherein (e) includes: for each said at least one password, the identification center simulating said encrypting on said each password using at least said encryption key, thereby creating at least one simulated encrypted password, and wherein (f) includes: the identification center associating each simulated encrypted password with a score indicating the matching degree between said received encrypted password and the respective simulated encrypted password; and the identification center selecting any simulated encrypted password having scores at least as good as a predetermined level; and wherein (g) includes: if in (f) a single simulated encrypted password is selected as having a score at least as good as said predetermined level, the identification center sending an indication that comparison results are sufficient to authenticate the user via said communication medium.

3. The method of claim 2, wherein a score as good as said predetermined level is indicative of a simulated encrypted password associated with said score being identical to said received encrypted password.

4. The method of any of the preceding claims, further comprising:

(h) the identification center receiving a preliminary identifier of the user, the identification center associating said preliminary identifier with less than all passwords accessible to the identification center, whereas said simulation in (e) on at least one password is performed on said associated less than all passwords.

5. The method of claim 4, wherein said preliminary identifier is associated with only one password, and said simulation in (e) on at least one password is performed on said only one password.

6. The method of any of claims 4 or 5, wherein said preliminary identifier includes at least one from a group including at least: a year of birth of the user, all digits in a national identification number of a user, less than all digits in a national identification number of a user, all digits in a social security number of a user, less than all digits in a social security number of a user, an expiry month and year of the user credit card, date of birth of a user, a name of the user, a personal identification number (PIN) of a user, maiden name of mother of user, city of birth of user, all digits in a credit card number of the user, less than all digits in a credit card number of the user, a predetermined number of digits along with a predetermined number of letters, all characters in a passport number, less than all characters in a passport number, all digits in a driver's license number, less than all digits in a driver's license number, all digits in a telephone number, less than all digits in a telephone number, all characters in an address, less than all characters in an address, and less than all characters in said password of the user.

7. The method of any of claims 4, 5 or 6, wherein said preliminary identifier is generated by the user.

8. The method of any of claims 4, 5 or 6, wherein said preliminary identifier is generated by an intermediate service provider based on enrollment data previously received from the user.

9. The method of any of claims 4 to 8, wherein said preliminary identifier is not associated with any passwords accessible to the identification center and therefore authentication of the user fails prior to (e).

10. The method of any of claims 1 to 3, wherein said simulation in (e) on at least one password is performed on all passwords accessible to the identification center.

11. The method of any of the previous claims, wherein said (a) includes: the identification center generating said encryption key and sending said encryption key to the user via the communication medium.

12. The method of any of claims 1 to 10, wherein said (a) includes: the user generating said encryption key and sending said encryption key to the identification center.

13. The method of any of claims 1 to 10, wherein (a) includes: an intermediate service provider generating said encryption key and sending said encryption key to the user and to the identification center.

14. The method of any of the previous claims, wherein said sent encryption key includes n and e and said password is substituted for X when calculating Y.

15. The method of any of the previous claims, wherein user authentication is desired prior to an intermediate service provider executing a transaction, further comprising: (i) an intermediate service provider generating a transaction identifier, said transaction identifier being used to distinguish a transmission over the communication medium relating to said transaction.

16. The method of any of the previous claims, wherein (c) includes: the user sending to an intermediate service provider said encrypted password and said intermediate service provider sending said encrypted password to the identification center, and wherein (d) includes: the identification center receiving said encrypted password from said intermediate service provider, and wherein (g) includes: if said comparison results are sufficient, the identification center providing to said intermediate service provider an indication that said comparison results are sufficient.

17. The method of any of the previous claims, wherein (c) includes: the user sending at least two encrypted passwords, at least one of said at least two to the identification center and at least one other of said at least two to an intermediate service provider, and wherein (d) includes: the identification center receiving said at least two encrypted passwords, said at least one of said at least two from the user and said at least one other of said at least two from said intermediate service provider, and wherein (e) and (f) are performed for each of said at least two received encrypted passwords, and wherein (g) includes: if all comparison results, associated with said at least two encrypted passwords are sufficient, the identification center providing an indication to said intermediate

service provider and an indication to the user that said all comparison results are sufficient.

18. The method of any of claims 16 or 17, wherein said indication of sufficiency provided by the identification center to said intermediate service provider includes a transaction identifier generated by said intermediate service provider, thereby enabling said intermediate service provider to execute a transaction for which authentication of the user is desired prior to execution.

19. The method of any of the previous claims, further comprising: (j) if said comparison results of (g) are insufficient, activating an action selected from a group that includes: (1) declaring failure, and (2) providing a new encryption key that includes at least one different element as stipulated in (a); and re-executing (a) to (g).

20. The method of any of the previous claims, wherein said password includes at least one predetermined user identification numbers selected from a group including at least: at least part of a credit card number of the user, at least part of a birth date of the user, at least part of a passport number of the user , at least part of a driving license number of the user, at least part of an address of the user, at least part of a phone number of the user, at least part of a social security number of the user, and at least part of a national identification number of the user.

21. The method of any of the preceding claims, wherein prior to (b), the user checks the validity of said encryption key sent in (a) and if invalid, (a) is repeated with a different encryption key.

22. The method of claim 21, wherein if said n is identical to a recently sent n to the user, said encryption key is invalid.

23. For use in the method of claim 1, limitations a, d, e, f, and g, a system for authenticating a user, through a user terminal, by an identification center, through an identification center terminal, the user terminal connected via a communication medium with the identification center terminal, the identification center terminal comprising:

(a) a receiver configured to receive an encrypted password via the communication medium from the user terminal or from an intermediate service provider terminal which is also connected via the communication medium, said encrypted password having been encrypted by the user terminal using an encryption key transmitted via the

communication medium, said encryption key including at least an n for applying a function $Y=X^e \pmod n$ to obtain said encrypted password;

(b) a storage configured to store passwords ;

(c) a simulator configured to simulate said encryption on at least one password from said storage;

(d) a comparator configured to compare said at least one simulated encrypted password to said received encrypted password; and

(e) a transmitter configured to transmit via the communication medium if said comparison results are sufficient to authenticate the user an indication that said comparison results are sufficient.

24. The system of claim 23, wherein said receiver is also configured to receive a preliminary identifier of the user and wherein said simulator is configured to simulate said encryption on each password in said storage which is associated with said preliminary identifier.

25. A system for authenticating a user through a user terminal, by an identification center, through an identification center terminal, the user terminal connected via a communication medium with the identification center terminal, the user terminal comprising:

(a) an encrypter configured to encrypt a password using at least an encryption key transmitted via the communication medium, said encryption key including at least an n for applying a function $Y=X^e \pmod n$ to said password;

(b) a transmitter configured to transmit said encrypted password to an intermediate service provider terminal which is also connected via the communication medium for transfer to the identification center terminal, or to transmit to the identification center terminal ; and

(c) a receiver configured to receive, if results of comparing said sent encrypted password with an encrypted password simulated by the identification center terminal are sufficient to authenticate the user, an indication that comparison results are sufficient.

26. A method for authenticating a user by an identification center, comprising:

(a) the identification center outputting an encryption key including at least an n for applying a function $Y=X^e(\text{mod } n)$ to a password of the user, wherein said password is presumed to be accessible to the user and to the identification center;

(b) the user encrypting said password using at least said encryption key;

(c) the user inputting said encrypted password to the identification center;

(d) the identification center simulating said encrypting on at least one of the passwords accessible to the identification center;

(e) the identification center comparing said at least one simulated encrypted password to said inputted encrypted password; and

(f) if results of said comparing are sufficient, the identification center outputting an indication that the user has been authenticated.

27. A system for authenticating a user, through a user terminal, by an identification center, through an identification center terminal, the identification center terminal comprising:

(a) an input configured to receive an encrypted password, said encrypted password having been encrypted by the user terminal using an encryption key outputted by the identification center terminal, said encryption key including at least an n for applying a function $Y=X^e(\text{mod } n)$ to obtain said encrypted password;

(b) a storage configured to store passwords ;

(c) a simulator configured to simulate an encryption on at least one password from said storage;

(d) a comparator configured to compare said at least one simulated encrypted password to said received encrypted password; and

(e) an output configured to output if said comparison results are sufficient to authenticate the user an indication that said comparison results are sufficient.

28. A system for authenticating a user through a user terminal, by an identification center, through an identification center terminal, , the user terminal comprising:

(a) an encrypter configured to encrypt a password using at least an encryption key outputted by the identification center terminal, said encryption key including at least an n for applying a function $Y=X^e(\text{mod } n)$ to said password;

(b) an output configured to output said encrypted password; and

(c) an input configured to receive, if results of comparing said outputted encrypted password with an encrypted password simulated by the identification center terminal are sufficient to authenticate the user, an indication that comparison results are sufficient, and configured to receive said encryption key.

29. A computer program product that includes a computer storage medium for storing a computer code portion for executing b and c of method claim 1.

30. A computer program product that includes a computer storage medium for storing a computer code portion for executing d, e, f, and g of method claim 1.

31. A computer program product that includes a computer storage medium for storing a computer code portion for executing b and c of method claim 26.

32. A computer program product that includes a computer storage medium for storing a computer code portion for executing a, d, e, and f of method claim 26.